Universidad Zaragoza
1542

Trabajo Fin de Grado

La Protección de Datos en un mundo cada vez más interconectado y complejo. Un estudio de la Protección de Datos en Derecho Internacional Privado dentro de la UE

Data Protection in an increasingly interconnected and complex world. A study of Data Protection in Private International Law within the EU

Autor/es

Guillermo Ortiz Pijuan

Director/es

Katia Fach Gómez

Facultad de Derecho

2020

Índice

1.- Presentación

El presente texto consiste en un análisis de los conceptos de privacidad y protección de datos dentro del ámbito de la Unión Europea. La decisión del tema fue prácticamente instantánea ya que se trata de un ámbito del derecho que siempre me ha resultado muy atractivo. El poder poner en conexión mis estudios en Derecho con un campo que siempre me ha gustado, como es el de la informática e Internet, es una buena manera de poner punto y final a este Grado.

Para la elaboración de este trabajo se ha consultado una extensa bibliografía, pero es cierto que ha facilitado en gran medida el hecho de haber tenido la oportunidad de cursar asignaturas como *Derecho de la Privacidad y Protección de Datos* o *Informática Legal* a través del Programa Erasmus en la Universidad de Laponia el pasado año. Haber tenido esta oportunidad me ha proporcionado una base teórica que ciertamente ha ayudado en el desarrollo del trabajo.

A continuación se exponen y se ponen en relación los conceptos de privacidad y protección de datos dentro de la normativa comunitaria de la Unión Europea, dando respuesta a cuestiones relacionadas con problemas de jurisdicción y ley aplicable. El objetivo de este trabajo es identificar las principales problemáticas surgidas del tratamiento de datos personales entre Estados Miembros, y de darles una respuesta lo más concisa posible apoyándome en las decisiones que la jurisprudencia comunitaria y nacional ha ido dictando.

2.- Introducción a la Sociedad de la Información

Ya llevamos décadas a nuestra espalda con Internet formando parte de nuestra vida. No solo ha servido para llevar al extremo la difusión y expansión del conocimiento a nivel mundial, sino que también ha sido una pieza clave en la instauración de una nueva manera de entablar relaciones contractuales a nivel global. Lo que denominamos "sociedad de la información", y que define toda esta situación global, ya no es ningún tipo de concepto nuevo e innovador, forma parte del presente y a mi juicio incluso, a un concepto desfasado y necesitado de actualización debido al rápido ritmo de evolución de nuestra sociedad en el ámbito tecnológico.

El término "sociedad de la información" se comenzó a utilizar en los años 60, dándose a conocer por el autor japonés Yoneji Masuda[1] a través de una obra de 1968, y desarrollándose en la restante segunda mitad del siglo XX. Pese a no existir una definición universal aceptada internacionalmente, la mayoría de autores se ponen de acuerdo para determinar que ésta apareció entre los años 70, las transformaciones del Bloque Socialista del Este en los 90 y los principios de los años 2000. En 1973 el autor Daniel Bell[2] introdujo el concepto de "sociedad de la información", con nociones muy básicas, y limitándose a teorizar que el eje principal de esta sociedad será el conocimiento teórico, pasando a ser los servicios basados en el conocimiento parte de estructura central de la nueva economía y de una nueva sociedad que se centra en la información. En los años 90 con el desarrollo de los ordenadores personales y el acceso a internet generalizado, este concepto de "sociedad de la información" vuelve a surgir con más fuerza[3], siendo incluida en la agenda de las reuniones del G7 en 1995. Posteriormente empezó a aparecer en foros de la Comunidad Europea y de la Organización para la Cooperación y el Desarrollo Económicos.

El autor Frank Webster [4] diferenciaba 5 tipos de información fundamentales: tecnológicos, económicos, ocupacionales, espaciales y culturales. Este trabajo va a centrarse en

[1] MASUDA, Y.: *Una introducción a la Sociedad de la Información*, Perikan-Sha, Tokio, 1968.

[2] BELL, D.: *El advenimiento de la sociedad post-industrial*, Alianza Editorial, 2006.

[3] BURCH, S.: *"Sociedad de la información/Sociedad del conocimiento*", en *Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información*, C & F Editions, 2005.

[4] WEBSTER, F.: *Information Society: Conception and Critique in Hall*, Encyclopedia of library and information science, Allen Kent y Carolyn M (editores), Suplemento 21. 58, New York, pp. 74–112, 1996.

esos tipos de información que conciernan a las relaciones de carácter privado en el ámbito internacional, que cada día aumentan y logran un mayor peso. La comunicación a través de Internet ha representado un desafío para el Derecho Internacional Privado, concretamente por la dependencia a unos factores de conexión geográfica. Un importante número de años han pasado, pero los autores de Derecho Internacional Privado siguen discutiendo acerca de si: a) se deben actualizar y reconsiderar algunos conceptos y normas relativas a Internet[5]; o si b) se trata de un "complejo problema de puesta en práctica"[6]. Pese a que las comunicaciones a través de Internet presentan unas particularidades que son complicadas de compaginar por normas de jurisdicción, muchos autores mantienen la opinión de que "no hay nada diferente o único acerca del ciberespacio que exija la modificación o abandono de los regímenes tradicionales de elección de derecho aplicable"[7].

[5] COLLINS*: The Law of Defamation and the Internet*, 3ª edn, OUP, 2010.

[6] MILLS: *Rethinking Jurisdiction in International Law*, BYbIntL, pp. 187, 197, 2004.

[7] SVANTESSO: *Private International Law and the Internet*, 2ª edn, Kluwer, pp. 52–62, 2013.

3.- Los conceptos de privacidad y protección de datos

3.1.- Introducción a los conceptos de privacidad y protección de datos

La definición de estos conceptos resulta complicada ya que su terminología cambia en cada entorno, cultura o legislación. A su vez, estas definiciones cambian y evolucionan con gran velocidad con los avances tecnológicos y de la sociedad. Las primeras apariciones de estas terminologías las encontramos en cuerpos legales tanto nacionales como internacionales desde los años 60, pero no pasarán a tomarse en serio adecuadamente hasta los años 90. Además, el hecho de que los dos conceptos se encuentren tan interconectados puede dificultar en alguna situación su separación. El derecho a la protección de datos se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, mientras que es el artículo 7 el que recoge el derecho al respeto a la vida privada y familiar. Este último derecho también está contenido en el artículo 8 de la Convención Europea de Derechos Humanos. Es el propio Reglamento General de Protección de Datos el que da una distinción entre los dos conceptos en su Considerando nº 4 al decir:

> *"(...) El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, (...)"*

El derecho a la privacidad puede considerarse más amplio que el de la protección de datos ya que cubre todos los asuntos relacionados con la vida personal y privada de un individuo. Es por ello que la protección de datos se encuentra dentro del ámbito de la privacidad[8], ya que se puede considerar "uno de los aspectos del derecho al respeto de la vida privada".

2.2.- Filtración de datos o "data breach"

Una filtración o violación de datos es un incidente de seguridad en el cual se accede a información sin autorización, pudiendo suponer importantes daños tanto para corporaciones

[8] HESS, B. y MARIOTTINI, C.: *Protecting Privacy in Private International and Procedural Law and by Data Protection: European and American Developments*, p. 83, 2015.

como para individuales. Con el avance y evolución de la tecnología, cada día se mueve más información en el mundo digital, y como consecuencia, los ciberataques se han vuelto más comunes y costosos. Según fuentes de la compañía de ciberseguridad Norton[9] (concretamente un estudio del instituto Ponemon), el coste medio para una gran empresa de estas filtraciones de datos se acerca a los 3,86 millones de dólares, y cada documento sustraído ronda un coste de 148 dólares. Esta realidad muestra que el cibercrimen en un peligro y una amenaza real para cualquier persona en internet. Los datos específicos que son robados con más frecuencia son nombres completos, números de tarjeta de crédito y números de Seguridad social, así como también cualquier tipo de información financiera. Estos ataques tienden a tener como objetivo a grandes empresas, ya que con un único ataque pueden llegar a recabar un gran número de datos. Lo que recogen las distintas leyes y regulaciones es una serie de pasos que tiene que seguir las compañías afectadas en caso de filtración de datos u otro incidente de seguridad similar. La gran parte de Estados obliga a dichas compañías a informar a sus clientes de aquellos datos que han sido o pueden estar comprometidos.

3.3.- Introducción a la regulación de la protección de datos

La regulación de la protección de datos está compuesta por una serie de normas que específicamente regulan todos o la mayoría de escenarios en el tratamiento de ciertos tipos de información. Estas normas determinan la manera en que la información en recogida, registrada, almacenada, usada y difundida. Por lo general, solamente la información personal es objeto de regulación por la normativa de protección de datos. Esta información personal o datos personales se definen como la información que permite la identificación de un individuo, ya sea persona natural o jurídica (referidos como individuos) o en ocasiones entidades colectivas. El objetivo principal de estas regulaciones es la protección de los intereses y derechos del individuo cuando información acerca del mismo está siendo tratada por un tercero. Estos intereses y derechos del individuo tienden a identificarse con los conceptos de privacidad, autonomía e integridad. Lee A.

[9] NORTON.COM, "What is a data breach?" Abril 2020.
https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

Bygrave[10] identifica una serie de principios centrales sobre los que se asientan todo cuerpo normativo de protección de datos:

1.- La información personal debe de ser recogida a través de medios justos y legales.

2.- La cantidad de datos personales recogidos debe de estar limitada a lo necesario para satisfacer la necesidad por la que se han recogido en primer lugar.

3.- La información personal debe ser recogida por finalidades específicas, legales y legítimas, y no debe de ser procesada de maneras incompatibles con esas finalidades.

4.- El uso y divulgación de información personal solo podrá realizarse para finalidades que ocurran con el consentimiento de la persona o personas a quien o quienes la información personal se refiera; o por la orden de una autoridad.

5.- La información personal debe de ser relevante, precisa y completa en relación a la finalidad para la que los datos se tratan.

6.- Deben tomarse medidas de seguridad con el fin de proteger dichos datos personales de divulgación, destrucción, modificación o uso no autorizados.

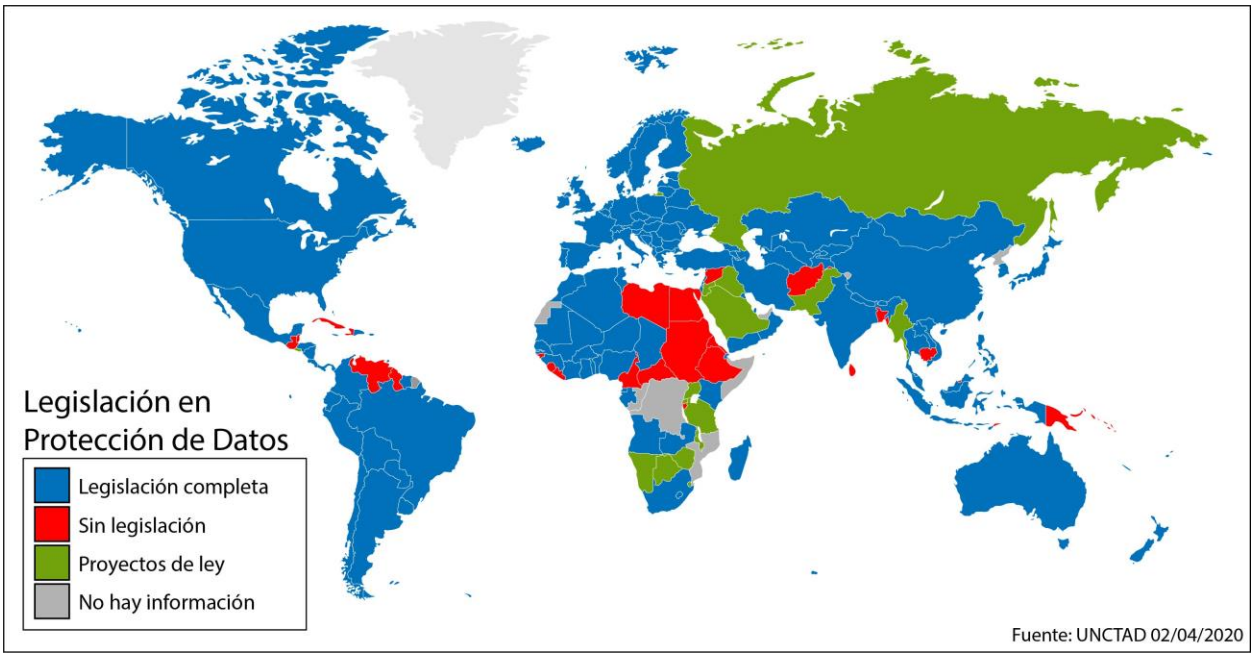
7.- Se debe informar a los interesados, además de dar acceso, a la información relativa a qué datos personales tienen terceros, así como a permitir rectificar estos datos si son imprecisos o incorrectos.

8.- Los responsables del tratamiento de la información deben responder del cumplimiento de las medidas que dan efecto a los principios anteriores.

La determinación de la jurisdicción y de la ley aplicable no es el único problema al que nos tenemos que enfrentar. Según las Naciones Unidas, solamente el 66% de las naciones del mundo tienen una legislación que regule todo lo relativo a la protección de datos. Un 10 % tienen proyectos de ley relativos a dicha regulación de protección de datos; un 19% no tiene una legislación específica para la protección de datos, o esta se encuentra sin regular; y un 5% de los países del mundo no han aportado información al respecto. A continuación se muestra un mapa en el que se pueden localizar las distintas regulaciones de protección de datos.

[10] BYGRAVE, L.A.: *Data Protection Law, Approaching its rationale, logic and limits*, Kuwer Law International 2009.

Legislación en Protección de Datos por países



Fuente: UNCTAD 02/04/2020[11]

Cabe recordar que no fue hasta los años 70 cuando se empezaron a redactar las primeras partes de lo que es hoy la legislación de protección de datos. Aparecieron nuevos instrumentos legales y cuasi-legales que dieron forma a lo hoy conocemos. De entre los primeros instrumentos internacionales, podemos destacar el Convenio del Consejo de Europa relativo a la Protección de los Individuos y respecto del Tratamiento de Datos Personales[12] (adoptada en enero de 1981); la Directiva 95/46/CE relativa a la Protección de Personas Físicas en lo respectivo al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (en vigor en noviembre de 1995); así como las Directrices de la OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales (adoptada en septiembre de 1980). Estos tres instrumentos tenían dos objetivos principales: contenían los principios básicos de protección de datos y servían de modelos para las distintas iniciativas legislativas que se han llevado posteriormente, ya sean internacionales o nacionales. Se volverá a hacer mención a la Directiva 95/45/CE más adelante, donde se

[11] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

[12] El Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos.

desarrollará con mayor detalle su función antes de la llegada del Reglamento General de Protección de Datos.

3.3.- ¿Derecho internacional privado o público?

Sigue presente el debate acerca de si la protección de datos pertenece al campo del Derecho Internacional Público o Privado, o en qué porcentaje pertenece a cada uno. Pese a no existir unanimidad acerca de este asunto, sí que se han pronunciado muchos autores a lo largo de los años y se ha llegado a una serie de conclusiones[13].

Si consideramos a la protección de datos como parte del derecho público exclusivamente, los juzgados y *Data Protection Authorities* siempre aplicarían su propio ordenamiento jurídico y nunca aplicarían ningún tipo de normativa extranjera o ajena a ese propio ordenamiento nacional. Aclarar si nos encontramos ante derecho público o privado es fundamental de cara a determinar si instrumentos de jurisdicción internacionales de gran importancia pueden ser de aplicación. El hecho de que tenga su origen en multitud de fuentes, y éstas sean muy diversas (Derechos Humanos, Derecho de Consumo, Derecho Mercantil,…), hace que sea imposible de categorizar como Derecho Internacional Público o Privado. El autor Jon Bing[14] estableció al respecto:

> *"La legislación de protección de datos generalmente contendrá disposiciones de naturaleza de derecho público, relacionadas con una autoridad y sus deberes y decisiones. Pero la ley también incluirá a menudo disposiciones de derecho civil, generalmente sobre responsabilidad por violaciones de protección de datos. Por lo tanto, las disposiciones de la legislación de protección de datos deben calificarse como pertenecientes a diferentes áreas del derecho, a las cuales se asignan diferentes criterios de conexión relevantes. Siguiendo el método tradicional, los diferentes aspectos de un caso pueden ser decididos por diferentes lex causae, lo que fácilmente conduce a confusiones, ya que la legislación se*

[13] KUNER, C.: *Data protection Law and International Jurisdiction on the Internet*, International Journal of Law and Information Technology, Vol. 18, p. 176, 2010.

[14] BING, J.: *Data Protection, Jurisdiction and the Choice of Law*, Privacy Law & Policy Reporter 92, 1999.

concibe como un todo orgánico donde las diferentes disposiciones respaldan una solución adecuada."[15]

Otras opiniones, como la del juez Lauterpacht[16], desprenden la idea de que no resulta útil ni merece la pena determinar si se trata de solamente Derecho Internacional Público o privado:

"Los derechos de las partes, especialmente en una disputa internacional, no deben determinarse por referencia a los controvertidos misterios de la distinción entre derecho privado y público".[17]

Se ha llegado a la conclusión de que no se debe darle tanta importancia a la manera de calificar al derecho de la protección de datos, y solo atender a su calificación dependiendo de la situación o caso. Por ejemplo, si una Autoridad de Protección de Datos ejercita una acción, ésta probablemente sea considerada como derecho público, mientras que si la acción es ejercitada por un actor privado, debe de ser consideraba como derecho privado (como por ejemplo la firma de un acuerdo de transferencia de datos entre entes privados).

El extendido uso de Internet por nuestra sociedad ha llevado a que algunas bases jurisdiccionales se fusionen o se vuelvan difíciles de distinguir. Mika Hayashi comenta en una de sus obras[18] que la diferencia entre el principio de territorialidad objetiva y las doctrinas de los efectos está desapareciendo debido a Internet, ya que el acto de dejar que un mensaje o información se vea en otro territorio y el efecto causado por él, se han vuelto difíciles de distinguir.

---

[15] Traducido del inglés: *"Data protection legislation will typically contain provisions of a public law nature, relating to an authority and its duties and decisions. But the law will also often include civil law provisions, typically on liability for data protection violations. The provisions of data protection legislation may therefore have to be qualified as belonging to different areas of law, to which different relevant connection criteria are assigned. Following the traditional method, different aspects of one case may then have to be decided by different lex causae, which is easily lead to distortions as the legislation is conceived as an organic whole where the different provisions support an appropriate solution."* (Original)

[16] Corte Internacional de Justicia, Rep 79, 86; relativa a un caso de aplicación del Convenio de 1902 sobre la guarda de menores (Boll Case).
https://www.icj-cij.org/files/case-related/33/033-19581128-JUD-01-00-EN.pdf

[17] Traducido del inglés*: "The rights of the parties, especially in an international dispute, ought not to be determined by reference to the controversial mysteries of the distinction between private and public law"* (Original)

[18] HAYASHI, M.: *The Information Revolution and the Rules of Jurisdiction in Public International Law*, The Resurgence of the State 59, 74-75, Ashgate, 2007.

3.4.- Distinción entre jurisdicción y conflicto de leyes

En Derecho Internacional Público se define el concepto de jurisdicción como "el derecho de un Estado bajo el Derecho Internacional para regular conductas en asuntos que no sean exclusivamente de interés interno"[19], mientras que este concepto contrasta con el de *choice of law* o conflicto de leyes, los cuales dan respuesta a la pregunta acerca de que legislación o legislaciones son de aplicación en cada caso de carácter internacional[20]. Pese a ser dos conceptos separados, estos están íntimamente relacionados, y con el paso del tiempo cada vez resulta más complejo diferenciarlos. Esta complejidad a la hora de diferenciarlos se acentúa en el campo de la protección de datos. La derogada normativa europea, la Directiva de Protección de Datos, en su artículo 4 hacía referencia a *national law applicable* o "legislación nacional aplicable", dando a entender que era una pura referencia al concepto de *choice of law*, determinando qué ley de protección de datos de un Estado Miembro era de aplicación en un caso concreto de tratamiento de datos personales. El hecho de que existiese un segundo artículo con normas específicas para jurisdicción (artículo 28.6), reforzaba la idea de que el artículo 4 solamente hacía referencia al *choice of law*. El citado artículo 28.6 asignaba la jurisdicción de las *DPAs* europeas entre ellas mismas. La realidad la muestra la práctica, donde bajo la derogada Directiva, las agencias nacionales de protección de datos solían equiparar jurisdicción y ley aplicable, algo que en ciertas ocasiones sigue ocurriendo a día de hoy con el Reglamento General de Protección de Datos.

Como ya se ha mencionado antes, en el área de la protección de datos la distinción entre normas de jurisdicción y de ley aplicable no resulta tan fácil. Esto se debe a que hay un importante elemento protector en el derecho de la protección de datos, que deriva de sus orígenes de la normativa de derechos humanos. Esto se refleja en el hecho de que tanto legisladores, como agencias de protección de datos o juzgados, se preocupan de asegurar que los datos personales no son privados de la protección de su propia legislación nacional una vez han sido transferidos fuera de su territorio.[21]

[19] OXMAN, B.: *Jurisdiction of States*, Encyclopedia of Public International Law, Vol. 3, Elsevier, 1997.

[20] MANN, F.A.: *Studies in International Law*, Claresdon Press Oxford, 2008.

[21] KUNER, C. Vid supra, nota 13.

4.- Protección de datos en la Unión Europea

4.1.- Mención a la regulación antes del Reglamento General de Protección de Datos

Antes de la llegada del Reglamento General de Protección de Datos en 2016, la norma existente era la Directiva de Protección de Datos[22] (Directiva 95/46/CE). Esta había sido adoptada en 1995 para regular el procesamiento de datos personales dentro de la Unión Europea. Esta Directiva no contenía ninguna norma relativa a la jurisdicción de los tribunales de los Estados Miembros respecto de acciones privadas, o por lo menos, no de manera explícita. Cierto es que el artículo 4 de esta Directiva regulaba específicamente qué Ley nacional era de aplicación en los procesamientos de datos personales, siendo norma general que la ley aplicable es la del Estado Miembro en el cual el controlador de datos tiene un establecimiento donde se procesan datos en el contexto de su actividad. Ésta facultaba a las *Data Protection Authorities*[23] *(DPAs)* para ejercer sus poderes en sus territorios incluso cuando la ley de otro Estado Miembro era de aplicación.

Con relación a las acciones o ejecuciones privadas, la jurisdicción de un tribunal normalmente no dependía de la lex fori[24]. La respuesta a la cuestión acerca de la jurisdicción sobre las acciones de aplicación privada que surgen de las leyes estatales que implementan la Directiva, la encontramos en las reglas generales sobre jurisdicción en Derecho Internacional Privado de los distintos Estados Miembros[25]. Estas reglas generales las encontrábamos en el Reglamento de Bruselas I[26], en la Convención de Lugano de 2007[27] y en las distintas reglas naciones de

[22] **Directiva 95/46/CE** del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[23] Las **Autoridades de Protección de Datos** son autoridades públicas independientes que supervisan la aplicación de la normativa de protección de datos a través de sus facultades de investigación y corrección. Existe una por cada Estado Miembro y por lo general, es el contacto de los Estados para preguntas acerca de protección de datos.

[24] **Lex fori:** en derecho internacional privado, expresión con la que se designa la ley del tribunal que entiende de la causa, tanto con referencia a las normas de derecho interno como a las de derecho internacional.

[25] LUNDSTEDT, L.: *International Jurisdiction Over Crossborder Private Enforcement Actions under the GDPR*, Stockholm Faculty of Law Research Paper Series nº 57, 2017.

[26] El **Reglamento de Bruselas I** determina los órganos jurisdiccionales de los distintos Estados miembros que son competentes para resolver litigios en materia civil y mercantil con un elemento internacional. Además, el Reglamento dispone que las resoluciones judiciales dictadas en un Estado miembro serán reconocidas en todos los Estados miembros sin necesidad de procedimiento especial alguno.

jurisdicción. Éstas últimas normalmente permitían al demandante elegir entre al menos dos (y en muchos casos incluso más) posibles lex fori.

Desde la perspectiva del tribunal del Estado Miembro, las reglas de jurisdicción contenidas en el Reglamento de Bruselas I eran de aplicación cuando el demandado reside en un Estado Miembro, además de que las normas de jurisdicción del Convenio de Lugano eran de aplicación para demandados en un estado suscrito al citado Convenio (Estados Miembro, Suiza, Islandia, Noruega y Dinamarca). Tanto el Reglamento como el Convenio son prácticamente idénticos, además de que eran interpretados de manera muy similar. Las normas de cada Estado Miembro también solían ser muy similares, aunque es cierto que tendían a ser más amplias y no tan genéricas. Por el contrario, si el demandado no se encontraba en ninguno de estos Estados mencionados, serán de aplicación las "normas del foro" o lex fori.

Las citadas normas de jurisdicción del Reglamento de Bruselas I estaban basadas en el principio *actor sequitur forum* (el demandado puede y debería ser demandado en su lugar de domicilio). Dicho reglamento incluía una definición del concepto de domicilio, la cual lo caracterizaba por ser una sede estatutaria, una administración central o el lugar principal donde se lleva a cabo un negocio. Este Reglamento utilizaba el mismo criterio que el artículo 54.1[28] del Tratado de Funcionamiento de la Unión Europea para definir el concepto de domicilio con el fin de determinar la nacionalidad de personas legales. El motivo por el que se usaba el mismo criterio de interpretación era para asegurar que no hubiese conflictos de jurisdicción donde a una persona jurídica con la nacionalidad de un Estado Miembro no se le diese la opción de estar domiciliada en otro estado Miembro.

4.2.- Introducción al Reglamento General de Protección de Datos

Este marco normativo fue el resultado de un proceso que dio comienzo en el año 2010 cuando el Consejo Europeo invitó a la Comisión Europea a evaluar el funcionamiento de la Unión Europea en relación a la protección de datos y a proponer nuevas iniciativas legislativas. Fue en la

[27] El **Convenio de Lugano** se firmó el 30 de octubre de 2007, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.

[28] La definición en el **artículo 54(1) del TFUE** se utiliza para determinar qué personas jurídicas disfrutan del derecho de libertad de establecimiento en relación con el artículo 49 y siguientes del Tratado de Funcionamiento de la Unión Europea.

resolución del Programa de Estocolmo[29] cuando el Parlamento Europeo ofreció una postura favorable a la elaboración de una nueva normativa, un régimen general para regular la protección de datos dentro de la Unión Europea. Se precisaba de un marco más amplio, sólido y actualizado a las necesidades y situación de la protección de datos. Se necesitaba fortalecer la seguridad jurídica de los ciudadanos europeos, operadores económicos y autoridades públicas; además de evitar la antes existente fragmentación en la aplicación de la protección de datos en el ámbito personal.

El 27 de enero de 2012 la Comisión Europea presentó una Propuesta de Reglamento relativa a la protección de las personas físicas en lo referente al tratamiento de datos personales, así como a la libre circulación de los mismos. Esta propuesta fue objeto de numerosas modificaciones a lo largo de 3 años, hasta que en fecha 15 de diciembre de 2015 el texto fue aprobado por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo. El texto legal fue finalmente publicado en el Diario Oficial de la Unión Europea[30] el día 4 de mayo de 2016, bajo el nombre de: Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Comúnmente se le denomina por las siglas RGPD o GDPR (por sus siglas en inglés).

El ámbito de aplicación material del Reglamento General de Protección de Datos se contiene en el artículo 2, en el cual se recoge que será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Además, se especifican una serie de supuestos al margen del ámbito de aplicación material, concretándose estas exclusiones para: el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea; a la actividad de las autoridades con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, además de la protección frente a amenazas a la seguridad pública; las actividades de los Estados Miembros comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de Funcionamiento de la UE; y por último, el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

[29] El **Programa de Estocolmo** fue un programa que establecía un plan de trabajo para el trabajo de la Unión Europea (UE) en el espacio de libertad, seguridad y justicia para el período 2010-2014.

[30] DOUE: L 119, 4.5.2016, p. 1–88
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

Respecto del ámbito de aplicación territorial, éste se contiene en el siguiente artículo, el 3. Será de aplicación al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea, independientemente de que el tratamiento tenga lugar en la Unión o no.

4.3.- Conflictos de competencia bajo el Reglamento General de Protección de Datos. La coexistencia del artículo 79.2 del GDPR y el artículo 7.2 del Reglamento de Bruselas I bis

Al contrario que en la Directiva de Protección de Datos, el Reglamento General de Protección de Datos tiene normas específicas de jurisdicción de los Estados Miembros para adjudicar demandas contra un encargado[31] o responsable[32] de datos que haya lesionado algún derecho de un interesado[33]. Es el artículo 79.2 el que permite que un interesado ejercite una acción en el Estado Miembro donde el responsable o encargado de datos tiene su establecimiento, o alternativamente en el Estado Miembro donde el interesado tiene su residencia habitual. La jurisdicción que dota el Reglamento General de Protección de Datos está limitada *ratione materiae* a demandas nacidas de derechos protegidos por el propio Reglamento. Solamente va a tener jurisdicción un Estado Miembro si el interesado interpone una demanda donde el Reglamento General de Protección de Datos sea la ley aplicable, y las actividades de tanto el responsable como el encargado deben caer en el alcance territorial del Reglamento. Estos responsables y encargados también deben de cumplir uno de los criterios del artículo 3.

El artículo 79.2 dispone que las acciones dirigidas contra encargados o responsables deben dirigirse ante los tribunales del Estado Miembro en el que tengan un establecimiento. Además,

[31] **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (artículo 4.8 RGPD).

[32] **Responsable del tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros (artículo 4.7 RGPD).

[33] **Interesado:** persona física identificada o identificable titular de los datos personales. Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (artículo 4.1 RGPD).

existe la posibilidad de ejercitar esas acciones en los tribunales competentes del Estado Miembro donde está el domicilio de la parte actora, siguiendo lo recogido en el Considerando nº 145 del Reglamento General de Protección de Datos. Estas acciones objeto del artículo 82 del Reglamento tienen un carácter "civil-mercantil"[34], lo que las encuadra dentro del ámbito de aplicación del Reglamento de Bruselas I bis, no estando en los supuestos de exclusión del artículo 1.2. En los casos de responsabilidad extracontractual con perjuicios originados por un tratamiento de datos ilícito según el artículo 82.6 del Reglamento General de Protección de Datos está muy claro que se ejercitan las acciones tal y como se acaban de describir. Cuando ese tratamiento de datos que genera el perjuicio se produzca dentro de una relación extracontractual: la jurisprudencia del Tribunal de Justicia de la Unión Europea establece que una acción de responsabilidad civil de naturaleza extracontractual deberá entenderse incluida en la materia contractual a los efectos del artículo 7 del Reglamento "Bruselas I bis" si el comportamiento recriminado comporta un incumplimiento de las obligaciones contractuales cuando se estudie caso por caso el objeto del contrato[35].

Por lo tanto nos encontramos con una norma que dicta que hay que ejercitar la acción ante el órgano jurisdiccional del lugar donde se haya producido o pueda producirse el hecho dañoso (Reglamento Bruselas I bis), y otra que nos recoge que también existe la posibilidad de demandar en el Estado Miembro donde reside el demandante (Considerando nº 145 del Reglamento General de Protección de Datos). La compatibilidad de las normas del Reglamento de Bruselas I bis y las del artículo 79.2 del Reglamento General de Protección de Datos deriva del artículo 67 del Reglamento de Bruselas I bis, ya que éste recoge que no prejuzgará la aplicación de las disposiciones contenidas en instrumentos particulares (como por ejemplo el artículo 79.2 GDPR). Pero el Considerando nº 147 del RGPD recoge que las normas generales de competencia judicial del Reglamento de Bruselas I bis deben entenderse sin perjuicio de la aplicación de las normas específicas del RGPD. Recordamos que el antes mencionado Considerando nº 145 recoge que el demandante debe tener la opción de ejercitar las acciones en los tribunales de los Estados Miembros.

---

[34] GONZALO DOMENECH, J.J. *Algunas cuestiones relevantes de derecho internacional privado del Reglamento General de Protección de Datos*, Rev. Boliv. De Derecho Nº 26, julio 2018, pp. 404-437.

[35] STJUE de 13 de marzo de 2014, Brogsitter, C-548/12, ECLI:EU:C:2014:148. http://curia.europa.eu/juris/document/document.jsf?text=&docid=149139&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=10544100

La respuesta a la cuestión de la coexistencia de las disposiciones de ambos cuerpos legales la encontramos tras el análisis de cada una de las disposiciones. La jurisdicción del Reglamento Bruselas I bis es más bien general y neutral, recogiendo foros para supuestos generales y no específicos ni concretos; mientras que lo recogido en el RGPD es más específico, más especial. Esta jurisdicción específica indica que ya hay algún tipo de conexión entre el foro y la cuestión jurídica a decidir; están presentes para adecuarse al supuesto concreto (tratamiento ilícito de datos personales que genera una responsabilidad extracontractual). Todo esto determina que el artículo 79.2 GDPR debe prevalecer sobre el artículo 7.2 del Reglamento de Bruselas I bis al ser más específico el primero.

Estando esto último claro, vamos a desarrollar lo recogido en el artículo 79.2 RGPD. Éste permite demandar en el Estado Miembro en el que el responsable de datos o encargado del tratamiento de datos tengan su establecimiento. Tal y como dice el autor Juan José Gonzalo Domenech[36], se debe tener un concepto flexible de "establecimiento". Esta idea se respalda por la jurisprudencia del TSJUE en casos como *Weltimmo*[37], donde se expresa que el concepto de establecimiento debe extenderse a cualquier actividad real y efectiva, aún mínima, ejercida mediante una instalación estable. Debe de tenerse en cuenta también lo que la sentencia comenta: el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión. En otra sentencia del STJUE, la relativa al caso *Amazon EU Sari*, se reconoce considerar la existencia de un establecimiento en un Estado Miembro cuando no exista no una filial o sucursal, debiendo valorarse el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en ese Estado Miembro. En este caso concreto, se permite considerar a un representante de la sociedad como establecimiento si actúa con un grado de estabilidad suficiente. Como ya se ha tratado antes, el Considerando nº 145 RGPD prevé un foro alternativo que permite a los afectados demandar en los tribunales del Estado donde tengan su residencia habitual. Cabe determinar en qué consiste ese concepto de "residencia habitual". La STJUE *Mercredi*[38] recogía

[36] GONZALO DOMENECH, J.J. Vid supra, nota 34.

[37] STJUE, Weltimmo, C-230/14 ECLI:EU:C:2015:639. http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=ES

[38] STJUE, Mercredi, C-497/10, ECLI:EU:C:2010:829. http://curia.europa.eu/juris/document/document.jsf?text=&docid=83470&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=10542825

que para considerar esta vía alternativa, es necesario que el afectado tenga un grado de permanencia en el Estado que muestre una situación de estabilidad.

4.4.- Ley aplicable. Relación con los Reglamento de Roma I y II

Es fundamental tener en cuenta que cuando analizamos un caso, tenemos que atender a la cláusula contractual correspondiente, la cual posiblemente delimita la ley aplicable. Es frecuente que estas cláusulas (las cuales tienen que atenerse a los criterios del RGPD) establezcan sujeciones a leyes de otros estados, de acuerdo con el Reglamento Roma I. Gonzalo Domenech[39] al explicar estas cláusulas pone de ejemplo las condiciones de Facebook España. Éstas recogen en su artículo 15.2 que cualquier litigio deberá resolverse aplicando las leyes del Estado de California en Estados Unidos, lo cual es acorde con el artículo 3.1 del Reglamento Roma I:

> *"El contrato se regirá por la ley elegida por las partes. Esta elección deberá manifestarse expresamente o resultar de manera inequívoca de los términos del contrato o de las circunstancias del caso. Por esta elección, las partes podrán designar la ley aplicable a la totalidad o solamente a una parte del contrato."*

Pero esta cláusula estará limitada por el artículo 6.2 del mismo Reglamento, el cual cita lo siguiente:

> *"No obstante lo dispuesto en el apartado 1, las partes podrán elegir la ley aplicable a un contrato que cumple los requisitos del apartado 1, de conformidad con el artículo 3. Sin embargo, dicha elección no podrá acarrear, para el consumidor, la pérdida de la protección que le proporcionen aquellas disposiciones que no puedan excluirse mediante acuerdo en virtud de la ley que, a falta de elección, habría sido aplicable de conformidad con el apartado 1."*

Esto significa que hay una obligación de estipular en el contrato entre las partes que las disposiciones legales que protegen al consumidor siguen siendo de aplicación al ser éste la parte "débil" de la relación contractual.

---

[39] GONZALO DOMENECH, J.J. Vid supra, nota 34.

La Sentencia del Tribunal de Justicia de la Unión Europea para el caso Amazon EU Sàrl[40], relativa a un caso procedente del Tribunal Supremo Civil y Penal austriaco entre la compañía Amazon y un particular, determina que:

> *"(…)una cláusula que figura en las condiciones generales que no ha sido negociada individualmente, en virtud de la cual la ley del Estado Miembro del domicilio social de ese profesional rige el contrato celebrado por vía de comercio electrónico con un consumidor, es abusiva en la medida en que induzca a error a dicho consumidor dándole la impresión de que únicamente se aplica al contrato la ley del citado Estado miembro, sin informarle de que le ampara también, en virtud del artículo 6, apartado 2, del Reglamento Roma I, la protección que le garantizan las disposiciones imperativas del Derecho que sería aplicable, de no existir esa cláusula, extremo que debe comprobar el órgano jurisdiccional nacional a la luz de todas las circunstancias pertinentes".*

En la práctica cuesta encontrar ejemplos que nos establezcan cual es la base jurídica para determinar la ley aplicable a cada caso en el ámbito de la protección de datos. Esto se debe a que importantes sentencias en el ámbito de la protección de datos no hacen demasiada referencia a estos aspectos. Por ejemplo, la conocida sentencia del Tribunal de Justicia de la Unión Europea para el caso Google Spain[41] no se refirió en ningún momento a los Reglamentos de Roma I y II, ni a la relación que tenían estos con el ya derogado artículo 4 de la Directiva de Protección de Datos. Podemos encontrar referencia a estos aspectos en jurisprudencia de otros estados miembros, concretamente Alemania, donde la sentencia una sentencia de un Tribunal de Schleswig-Holstein[42] (relativa a un supuesto de determinación de ley de protección de datos aplicable a un contrato de términos y servicios de Facebook) determinó que era de aplicación la ley de protección de datos del Estado Miembro donde se establece la filial europea encargada del tratamiento de datos (en el caso, Irlanda), y no la del Estado Miembro donde se establece la filial encargada de los servicios publicitarios (en el caso, Alemania).

---

[40] STJUE de 28 de julio de 2016, Amazon EU Sàrl, C-191/15, EU:C:2016:612. http://curia.europa.eu/juris/document/document.jsf?text=&docid=182286&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=10542912

[41] STJUE de 20 de junio de 2014, Google Spain, C-131/12. http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

[42] VG Schleswig-Holstein, Beschluss vom 14.02.2013, Az. 8 B 60/12. https://www.datenschutzzentrum.de/uploads/facebook/Facebook-Ireland-vs-ULD-Beschluss.pdf

Para las disputas englobadas en la responsabilidad extracontractual, debemos atender a un texto legal diferente previsto para estos casos: el Reglamento Roma II. Antes de entrar más en el fondo de este texto, debemos atender a su artículo 1.2g, el cual excluye de su aplicación "las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad". Esto significa que van a estar excluidas de esta norma cualquier vulneración de los derechos protegidos por la normativa de protección de datos consecuencia del tratamiento de datos de un encargado o responsable. La manera a proceder en estos casos es atender a normas autónomas como es el artículo 10.9 del Código Civil español:

"Las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven (…)".

A esta norma se le denomina *lex loci delicti commissi,* y puede resultar sencilla su aplicación para casos en los que los elementos constitutivos de acto y resultado están en el mismo Estado. La problemática surge cuando entramos en el ámbito del Derecho de la Protección de Datos, donde es más que frecuente que estos elementos constitutivos están en lugares distintos[43]. Para dar salida a esta problemática debemos atender a las dos posibilidades que nos presenta el citado artículo 10.9 CC: aplicar la ley del lugar donde se produce el daño para la victima (denominada *lex loci damni*), o aplicar la ley del lugar en el que efectivamente se produce el hecho o acto del que deriva la responsabilidad (denominada *lex loci actus*).

Respecto de esta segunda opción, la *lex loci actus*, debemos tener en cuenta que en la mayoría de los casos el hecho ilícito deriva de una cadena de ilícitos desarrollada a través de varios Estados. "El tratamiento automatizado de datos personales se rige por la ley del Estado en cuyo territorio tiene lugar dicho tratamiento de datos que ha provocado el daño"[44]. Por lo tanto, para que se pudiese aplicar la ley española en un caso, se precisaría que el responsable del fichero de datos tenga su domicilio fuera de la UE y el tratamiento de datos se realice en España. En relación a la *lex loci damni*, "debe rechazarse que cualquier lugar de recepción de los contenidos o la información transmitidos por Internet sea por esa simple circunstancia lugar del daño[45]". Esto se justifica por el hecho de que ese acto no suele generar un daño real a la víctima, además de que si se

[43] DE MIGUEL ASENSIO, P.A.: *Derecho Privado de Internet*, Civitas, Madrid, 8ª Edición , 2015.

[44] ORTEGA GIMENEZ, A.*: La (des)Protección del Titular del Derecho a la Protección de Datos Derivada de una Transferencia Internacional Ilícita*, AEPD, Madrid, 2015, p.143.

[45] GONZALO DOMENECH, J.J. Vid supra, nota 34.

aplicase la ley de cada sitio donde se ha manifestado, favoreceríamos una fragmentación normativa excesiva.

4.5.- Las transferencias internacionales de datos y las *cross-border situations*

Podemos definir una trasferencia internacional de datos como un tratamiento de datos que suponga una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en España. A la hora de tratar este concepto introducido en el Reglamento General de Protección de Datos, debemos atender a la reciente jurisprudencia del Tribunal de Justicia de la Unión Europea, ya que ésta ha sido de especial trascendencia y ha tenido una importante incidencia en el RGPD. La STJUE de 6 de octubre de 2015, asunto C-362/14, estima que la existencia de una decisión de la Comisión que declara a un país tercero con un nivel de protección adecuado de los datos personales transferidos no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control.

La cuestión a tratar a continuación es qué situaciones derivadas de una transferencia internacional de datos se encuentran dentro del alcance del Reglamento General de Protección de Datos. La autora Anni-Maria Taka[46] habla de *cross-border situations* para referirse a estos casos. El artículo 3 del Reglamento es de aplicación en principio cuando el responsable o encargado de tratamiento de datos no están presentes en la Unión Europea y el interesado está presente físicamente en la Unión. Pero no para todos los casos, ya que el segundo punto del artículo 3 especifica que el RGPD será de aplicación para actividades de tratamiento relacionadas con: la oferta de bienes o servicios a dichos interesados en la Unión, o el control de su comportamiento, en la medida en que este tenga lugar en la Unión. Esto es desarrollado por el Considerando nº 23 del RGPD:

> *"Con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de interesados que residen en la Unión por un responsable o un encargado no establecido*

[46] TAKA, A.M.: *Cross-Border Application of EU's General Data Protection Regulation* – A Private International Law study on Third State Implications, Uppsala University, Master's Thesis in Private International Law and EU Law, 2017.
http://www.diva-portal.org/smash/get/diva2:1127596/FULLTEXT01.pdf

en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión."

5.- Conclusión

El rápido desarrollo de la tecnología provoca que nuestra sociedad necesariamente evolucione y se adapte a los nuevos escenarios que se presentan. Tal y como y como dice Tobias Lutzi[47], la comunicación a través de Internet se caracteriza por su: ubicuidad, así como por su virtualidad. Esto significa que cada caso es conducido a una multiplicación de conexiones en distintos lugares físicos. Da la sensación de que en el ámbito tecnológico, el Derecho va un paso por detrás, tratando de remediar problemas que existían ayer, para que pasado mañana se encuentre con nuevos. Es inevitable esta situación, ya que los procesos legislativos requieren de mucho tiempo para que se lleven a cabo de la manera adecuada.

En este sentido, podemos considerar que el Reglamento General de Protección de Datos ha supuesto un gran paso para la Unión Europea, actualizando esos nuevos escenarios, dando un nuevo nivel de protección a la ciudadanía y coordinando el funcionamiento de la protección de datos a nivel europeo. La alternativa que brinda el RGPD al interesado para ejercitar acciones directamente contra el responsable o encargado de tratamiento de datos en el Estado Miembro en el que tenga su residencia habitual, ha permitido reforzar y darle poder al interesado para tener más control sobre sus derechos.

[47] LUTZI, T.: Internet Cases in EU Private International Law Developing a Coherent Approach, International & Comparative Law Quarterly, 2017

Bibliografía

Monografías:

- BELL, D.: *El advenimiento de la sociedad post-industrial*, Alianza Editorial, 2006.
- BYGRAVE, L.A.: *Data Protection Law, Approaching its rationale, logic and limits*, Kuwer Law International, 2009.
- COLLINS: *The Law of Defamation and the Internet*, 3ª edn, OUP, 2010.
- HAYASHI, M.: *The Information Revolution and the Rules of Jurisdiction in Public International Law*, The Resurgence of the State 59, Ashgate, 2007.
- HESS, B. y MARIOTTINI, C.: *Protecting Privacy in Private International and Procedural Law and by Data Protection: European and American Developments*, Routledge, 2015.
- MANN, F.A.: *Studies in International Law*, Claresdon Press Oxford, 2008.
- MASUDA, Y.: *Una introducción a la Sociedad de la Información*, Perikan-Sha, Tokio, 1968.
- MILLS: *Rethinking Jurisdiction in International Law*, BYbIntL, 2004.
- ORTEGA GIMENEZ, A.*: La (des)Protección del Titular del Derecho a la Protección de Datos Derivada de una Transferencia Internacional Ilícita*, AEPD, Madrid, 2015.
- SVANTESSO*: Private International Law and the Internet*, 2ª edn, Kluwer, 2013.
- TAKA, A.-M.: *Cross-Border Application of EU's General Data Protection Regulation – A Private International Law study on Third State Implications*, Uppsala University, Master's Thesis in Private International Law and EU Law, 2017.

Capítulos de libros:

- BING, J.: *Data Protection, Jurisdiction and the Choice of Law*, Privacy Law & Policy Reporter 92, 1999.
- BURCH, S.: *Sociedad de la información/Sociedad del conocimiento*, en *Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información*, C & F Editions, 2005.

- GONZALO DOMENECH, J.J.: *Algunas Cuestiones Relevantes de Derecho Internacional Privado del Reglamento General de Protección de Datos*, Rev. Boliv. De Derecho Nº 26, ISSN: 2070-8157, pp. 404-437, julio 2018.
- GONGOL, T. y ZAHRADNÍKOVÁ, R.: *International Court Jurisdiction in Disputes Concerning Unlawful Use of Trademarks on the Internet*, DANUBE: Law, Economics and Social Issues Review, 10 (1), pp. 91-102, 2019.
- JUMA'H, A. y ALNSOUR, Y.: *The Effect of Data Breaches on Company Performance*, International Journal of Accounting & Information Management Vol. 28 nº 2, 2020, pp. 275-301, Emerald Publishing Limited, 2020.
- OXMAN, B.: *Jurisdiction of States*, Encyclopedia of Public International Law, Vol. 3, Elsevier, 1997.
- SEGURA-SERRANO, A.: *Internet Regulation and the Role of International Law*, Max Planck Yearbook of United Nations Law, Volume 10, pp. 191-271, 2006.
- WEBER, F.: *Information Society: Conception and Critique in Hall*, Encyclopedia of library and information science, Allen Kent y Carolyn M (editores), Suplemento 21. 58, New York, pp. 74–112, 1996.

Artículos y documentos:

- BRKAN, M.: *Data Protection and European Private International Law*, EUI Working Paper Robert Schuman Centre for Advances Studies 2015/40, Florence School of Regulation, 2015.
- CORLEY, M.: *The Need for an International Convention on Data Privacy: Taking a Cue from the CISG*, Brooklyn Journal of International Law, Vol. 41, Issue 2, Article 5, 2016
- JERKER B. SVANTESSON, D.: *A Vision for the Future of Private International Law and the Internet*, Harvard ILJ, 2019.
- KATUNINA, M. y VERCHANKO, O.: *Internet Law in International Private Law*, Rezekne Academy of Technologies, 2019.
- KUNER, C.: *Data protection Law and International Jurisdiction on the Internet*, International Journal of Law and Information Technology, Vol. 18, 2010.

- LITTLE, L.: *Internet Defamation, Freedom of Expression, and the Lessons of Private International Law for the United States*, Legal Studies Research Paper Series Nº 2013-03, Beasley School of Law, Temple University, 2013.
- LUNDSTEDT, L.: *International Jurisdiction Over Crossborder Private Enforcement Actions under the GDPR*, Stockholm Faculty of Law Research Paper Series nº 57, 2017
- LUTZI, T.: *Internet Cases in EU Private International Law Developing a Coherent Approach*, International & Comparative Law Quarterly, 2017.
- LOPEZ-LAPUENTE, L. y BERMEJO BOSCH, R.: *Business-focused Legal Analysis and Insight in the Most Significant Jurisdictions Worldwide: Spain*, The Privacy, Data Protection and Cybersecurity Law Review- Edition 6, octubre 2019.
- MAYOR GOMEZ, R.: *Contenido y Novedades del Reglamento General de Protección de Datos de la UE*, GABILEX Nº6, junio 2016.
- MENDOZA LOSANA, A.I.: *Transferencias Internacionales de Datos Personales: Estados Unidos no es un Puerto Seguro, pero tampoco una Isla Inalcanzable*, Centro de Estudios de Consumo, Universidad de Castilla-La Mancha, 2015.
- NIEUWESTEEG, B. y FAURE, M.: *An Analysis of the Effectiveness of the EU Data Breach Notification Obligation*, Erasmus University Rotterdam, 2018.
- NOLAN, K.: *GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law*, Berkeley Technology Law Journal, University of California, Berkeley School of Law, 2018.
- PERNOT-LEPLAY, E.: *Data Privacy Law in China: A Third Way Between the US and the EU?*, Penn State Journal of Law and International Affairs, vol. 8.1, 2020.
- PRIVACY RIGHTS CLEARINGHOUSE: *Data Breach Notification in the United States and Territories*, 2018
- RADU, R.: *Negotiating Internet Governance*, Oxford University Press, 2019
- SVANTESSON, D.: *Time for International Law to take the Internet Seriously*, Oxford University Press, 2020.
- VAN CALSTER, G.: *On Soggy Grounds. The GDPR and Jurisdiction for Infringement of Privacy*, L'Observateur de Bruxelles, julio 2018.
- VERMEULEN, G. y LIEVENS, E.: *Data Protection and Privacy under Pressure. Transatlantic Tensions, EU Surveillance and Big Data*, Marklu, 2017.

- VON HEIN, J.: *Social Media and the Protection of Privacy*, European Data Science Conference, Luxembourg, noviembre 2016.

Jurisprudencia comunitaria y nacional:

- Sentencia del Tribunal de Justicia de la Unión Europea de 20 de mayo de 2010, *Ceská podnikatelská v. Michal Bilas*, C-111/09.

https://op.europa.eu/es/publication-detail/-/publication/21e3461c-f523-4b62-8834-295cafb1b62c

- Sentencia del Tribunal de Justicia de la Unión Europea de 22 de diciembre de 2010, *Mercredi*, C-497/10.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=83470&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=10542825

- Sentencia del Tribunal de Justicia de la Unión Europea de 25 de octubre de 2011, *eDate Advertising*, C-509/09.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=10545337

- Sentencia del Tribunal de Justicia de la Unión Europea de 3 de octubre de 2013, *Pickney*, C-170/12.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=142613&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=10547673

- Sentencia del Tribunal de Justicia de la Unión Europea de 13 de marzo de 2014, *Brogsitter*, C- 548/12.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=149139&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=10544100

- Sentencia del Tribunal de Justicia de la Unión Europea de 20 de junio de 2014, *Google Spain*, C-131/12.

http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

- Sentencia del Tribunal de Justicia de la Unión Europea de 28 de enero de 2015, *Kolassa*, C-375/13.

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOC_2015_107_R_0004&from=ES

- Sentencia del Tribunal de Justicia de la Unión Europea de 1 de octubre de 2015, *Weltimmo*, C-230/14.

http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=ES

- Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015, *Schrems*, C-362/14.

http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES

- Sentencia del Tribunal de Justicia de la Unión Europea de 14 de julio de 2016, *Granarolo*, C-196/15.

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62015CJ0196

- Sentencia del Tribunal de Justicia de la Unión Europea de 21 de diciembre de 2016, *Amazon EU Sarl*, C-362/14.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=182286&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=10542912

- Sentencia del Tribunal de Justicia de la Unión Europea de 25 de enero de 2018, *Schrems vs Facebook*, C-498/16.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=198764&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=10547866

- VG Schleswig-Holstein, Beschluss vom 14.02.2013, Az 8 B 60/12.

https://www.datenschutzzentrum.de/uploads/facebook/Facebook-Ireland-vs-ULD-Beschluss.pdf

Legislación comunitaria y nacional:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos (RGPD)
- Reglamento (CE) No 593/2008 del Parlamento Europea y del Consejo, de 17 de junio de 2008 sobre la ley aplicable a las obligaciones contractuales (Roma I)
- Reglamento (CE) n° 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007 , relativo a la ley aplicable a las obligaciones extracontractuales (Roma II)
- Reglamento (UE) Nº 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Bruselas I bis)

- Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.